



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Ching-Jun Su, et al. )  
Serial No.: 10/052,755 )  
Filed: January 18, 2002 ) Our Ref: B-4467 619464-5  
For: "WIRELESS FINGERPRINT IDENTITY )  
APPARATUS AND METHOD" ) Date: June 17, 2002

CLAIM TO PRIORITY UNDER 35 U.S.C. 119 RECEIVED

JUN 27 2002

Honorable Commissioner of Patents and Trademarks  
Washington, D.C. 20231

Technology Center 2100

Sir:

[X] Applicant hereby makes a right of priority claim under 35  
U.S.C. 119 for the benefit of the filing date(s) of the  
following corresponding foreign application(s):

<u>COUNTRY</u>	<u>FILING DATE</u>	<u>SERIAL NUMBER</u>
TAIWAN, R.O.C.	16 November 2001	90128526

[ ] A certified copy of each of the above-noted patent  
applications was filed with the Parent Application  
No. \_\_\_\_\_.

[X] To support applicant's claim, a certified copy of the above-  
identified foreign patent application is enclosed herewith.

[ ] The priority documents will be forwarded to the Patent Office  
when required or prior to issuance.

I hereby certify that this correspondence  
is being deposited with the United States  
Postal Service with sufficient postage as  
first-class mail in an envelope addressed  
to the "Commissioner of Patents and  
Trademarks, Washington, D.C. 20231",  
on June 17, 2002 by Courtney Comstock.

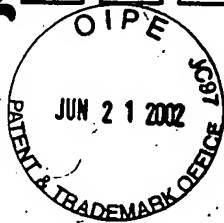
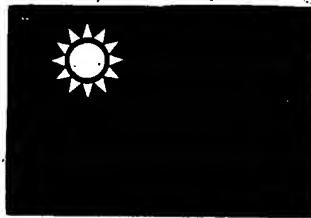
*Courtney Comstock*

Respectfully submitted,

*Richard P. Berg*  
Richard P. Berg  
Attorney for Applicant  
Reg. No. 28,145

LADAS & PARRY  
5670 Wilshire Boulevard  
Suite 2100  
Los Angeles, CA 90036  
Telephone: (323) 934-2300  
Telefax: (323) 934-0202

10/052,755



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE  
MINISTRY OF ECONOMIC AFFAIRS  
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，  
其申請資料如下：

This is to certify that annexed is a true copy from the records of this  
office of the application as originally filed which is identified hereunder.

申請日：西元 2001 年 11 月 16 日  
Application Date

申請案號：090128526  
Application No.

申請人：宏基電腦股份有限公司  
Applicant(s)

RECEIVED

JUN 27 2002

Technology Center 2100

RECEIVED

JUN 27 2002

Technology Center 2600

局長  
Director General

CERTIFIED COPY OF  
PRIORITY DOCUMENT

陳明邦

發文日期：西元 2002 年 4 月 22 日  
Issue Date

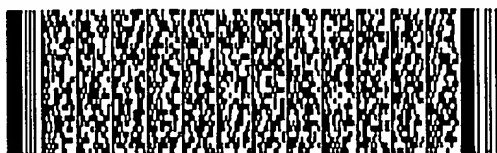
發文字號：09111006764  
Serial No.

申請日期：	案號：
類別：	

(以上各欄由本局填註)

## 發明專利說明書

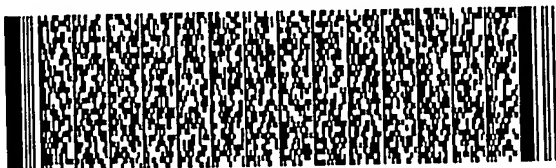
一、 發明名稱	中 文	無線指紋辨識裝置
	英 文	
二、 發明人	姓 名 (中文)	1. 賴世勤 2. 蔡竹嘉 3. 蘇進榮
	姓 名 (英文)	1. 2. 3.
	國 籍	1. 中華民國 2. 中華民國 3. 中華民國
	住、居所	1. 台北縣汐止市新台五路一段88號21樓 2. 台北縣汐止市新台五路一段88號21樓 3. 台北縣汐止市新台五路一段88號21樓
三、 申請人	姓 名 (名稱) (中文)	1. 宏碁電腦股份有限公司
	姓 名 (名稱) (英文)	1. Acer Incorporated
	國 籍	1. 中華民國
	住、居所 (事務所)	1. 台北縣汐止市新台五路一段八十八號二十一樓
	代表人 姓 名 (中文)	1. 施振榮
	代表人 姓 名 (英文)	1.



四、中文發明摘要 (發明之名稱：無線指紋辨識裝置)

本發明係一種電子系統之無線指紋辨識裝置，包括：  
一識別器，具有指紋擷取模組，其耦接於射頻模組，可取得使用者的指紋資料，並透過上述射頻模組以一無線傳輸協定傳送指紋資料。一接收模組，可接收透過無線傳輸協定所傳送之該指紋資料；以及一指紋鑑別模組，耦接於接收模組及記憶體，其中上述接收模組，可接收由無線傳輸協定所傳送之指紋資料。若指紋鑑別模組比對指紋資料與預設指紋資料相符時，則開放電子系統之使用權。若指紋鑑別模組比對指紋資料與預設指紋資料不相符時，則關閉電子系統。

英文發明摘要 (發明之名稱：)



本案已向

國(地區)申請專利

申請日期

案號

主張優先權

無

有關微生物已寄存於

寄存日期

寄存號碼

無

## 五、發明說明 (1)

本發明係有關於一種指紋辨識裝置及其方法，特別係有關一種利用藍芽無線傳輸協定之無線指紋辨識裝置及其方法。

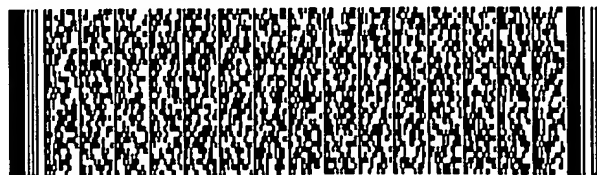
以往，我們在操作電腦時，尤其是操作多人使用的電腦或是較機密的電腦時，通常會要求使用者輸入使用者識別碼及身份認證密碼等，透過這種保密機制來限制使用者的系統使用權限，或是來達到系統管理的目的；但是使用者識別碼及身份認證密碼也有外洩的可能，若被不法人士取得，所有的機密資料都將會有洩露之虞，對於真正儲存機密資料的系統來說，僅使用識別密碼的認證程序，對於機密系統的資料安全防護來說是非常薄弱的。

後來有人發展出以IC卡搭配身份認證密碼使用，可為系統增加一層安全防護，避免因為密碼被不法人士取得，造成機密資料遺失。雖然以IC卡搭配身份認證密碼使用，可為系統增加一層安全防護，但是由於人的疏忽，往往會因為不注意時，忘記將IC卡帶走，這樣更增加安全上的漏洞。

對於這種機密電腦系統的身份識別問題，若使用每個人身上都有且均不相符的指紋，就可很簡單達到身份確認的工作。

以現有的技術來說，一般我們所看到的指紋辨識裝置，通常是桌上型個人電腦另以一外接方式連結外接式指紋辨識裝置，來達到辨識使用者身份的需求。

請參考第1圖，第1圖係表示根據習知技術中，外接式



## 五、發明說明 (2)

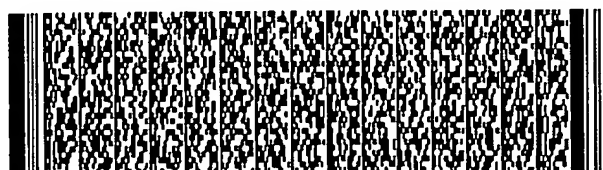
指紋辨識器之示意圖，當使用者要進行指紋辨識時，需將外接式指紋辨識器13透過連接纜線14連接個人電腦11，再由指紋擷取模組12取得使用者之指紋資料以進行比對。

請參考第2圖，第2圖係表示根據習知技術中，使用外接式指紋辨識器之身份識別方法流程圖。

如第2圖所示之步驟，使用者或系統管理者於桌上型個人電腦11上建立預設指紋資料(步驟S201)，這項動作可能是以一安裝軟體的方式來達成，並將上述的預設指紋資料儲存於個人電腦11中，以完成建檔工作。

當使用者要使用該桌上型個人電腦11時(步驟S202)，使用者將指紋辨識器13透過連接纜線14連接到個人電腦11上(步驟S203)，系統會要求使用者輸入指紋資料，此時使用者將手指置於指紋擷取模組12上，該指紋擷取模組12取得使用者的指紋後，將指紋資料傳送至個人電腦11後，個人電腦11會判斷所輸入之指紋資料是否正確?(步驟S204)，若所輸入之指紋資料與預設指紋資料相符時，則開放個人電腦11之使用權(步驟S205)；若所輸入之指紋資料與預設指紋資料不同時，則鎖住或關閉該個人電腦11(步驟S206)，最後完成上述的身份識別程序(步驟S207)。

但是，這對於許多使用筆記型電腦或數位個人行動助理(PDA)的商務人士來說，這種外接式指紋辨識器13除了攜帶及使用不方便外，在外出開會時，通常在筆記型電腦中也會儲存一些未定案的資料或是機密資料，這些通常都



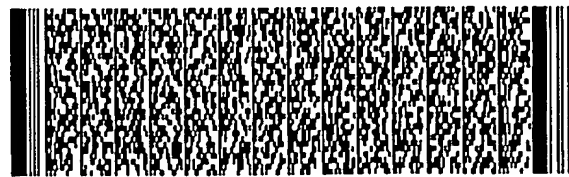
### 五、發明說明 (3)

是不希望客戶看到的，所以在使用筆記型電腦前還拿出外接式指紋辨識器13辨識使用者指紋，這種動作會被解釋成對客戶的一種不信任，但不如此做的話又怕筆記型電腦遺失，機密資料外洩，這可能會造成企業莫大的損失。

有鑑於此，本發明的目的就在於提供一種使用無線傳輸協定的指紋辨識裝置，該指紋辨識裝置具有一無線指紋識別器，可透過無線電將使用者指紋資料傳送給一接收端，以控制電子裝置的使用權。

為達成上述目的，本發明實施例提供一種電子系統之無線指紋辨識裝置，包括：一識別器，具有指紋鑑別模組耦接於指紋擷取模組、射頻模組及記憶體，其中上述指紋擷取模組可取得使用者的指紋資料，記憶體用以儲存一預設指紋資料，若指紋鑑別模組比對輸入之指紋資料與預設指紋資料相符時，可透過射頻模組以藍芽無線傳輸協定傳送一控制訊號；以及一接收模組，用以接收該無線傳輸協定所傳送之控制訊號，並啟動上述電子系統或開放上述電子系統之使用權。

本發明實施例另提供一種電子系統之無線指紋辨識裝置，包括：一識別器，具有指紋擷取模組，其耦接於射頻模組，可取得使用者的指紋資料，並透過上述射頻模組以一無線傳輸協定傳送指紋資料；一接收模組，可接收透過無線傳輸協定所傳送之該指紋資料；以及一指紋鑑別模組，耦接於接收模組及記憶體，其中上述接收模組，可接收由無線傳輸協定所傳送之指紋資料。若指紋鑑別模組比





#### 五、發明說明 (4)

對指紋資料與預設指紋資料相符時，則開放電子系統之使用權；若指紋鑑別模組比對指紋資料與預設指紋資料不相符時，則關閉電子系統。

依據本發明實施例之無線指紋辨識裝置，提供一種無線身份識別方法，包括下列步驟：預先設定一預設指紋資料，在取得一指紋資料後，比對預設指紋資料與上述指紋資料，若該指紋資料與預設指紋資料相符時，則透過一無線通訊協定傳送一控制訊號，其中，該控制訊號可用來啟動一電子系統或開放其使用權。

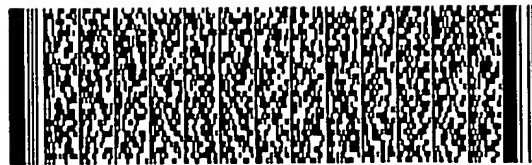
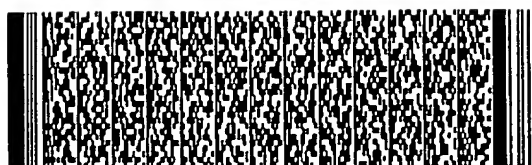
依據本發明實施例之無線指紋辨識裝置，提供另提供一種無線身份識別方法，包括下列步驟：預先設定一預設指紋資料，在取得一指紋資料後，透過一無線通訊協定傳送該指紋資料；經比對預設指紋資料與上述指紋資料後，若該指紋資料與預設指紋資料相符時，則送出一控制訊號，其中，該控制訊號可用來啟動一電子系統或開放其使用權。

為了讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖示，作詳細說明如下：

圖式簡單說明：

第1圖係表示根據習知技術中，外接式指紋辨識器之示意圖。

第2圖係表示根據習知技術中，使用外接式指紋辨識器之身份識別方法流程圖。



## 五、發明說明 (5)

第3圖係表示根據本發明實施例中，具有無線指紋辨識裝置之筆記型電腦示意圖。

第4A圖係表示根據本發明實施例中，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

第4B圖係表示根據本發明實施例中，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

第5A圖係表示根據本發明第二實施例中，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

第5B圖係表示根據本發明第二實施例中，具有無線指紋辨識裝置之筆記型電腦，另一實施方式之系統方塊圖。

第5C圖係表示根據本發明第二實施例，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

第6A圖係表示根據本發明第三實施例，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

第6B圖係表示根據本發明第三實施例，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

符號說明：

11~ 桌上型個人電腦

12~ 指紋擷取模組

13~ 外接式指紋辨識器

14~ 連接纜線

20~ 識別器

21~ 指紋擷取模組

22~ 射頻模組



## 五、發明說明 (6)

- 23~ 識別器之指紋鑑別模組
- 24~ 識別器之記憶體
- 30~ 筆記型電腦
- 31~ 接收模組
- 32~ 筆記型電腦內部晶片組
- 33~ 電源供應器
- 34~ 指紋鑑別模組(筆記型電腦內)
- 35~ 記憶體(筆記型電腦內)
- 36~ 筆記型電腦之中央處理單元
- 40~ 無線電波

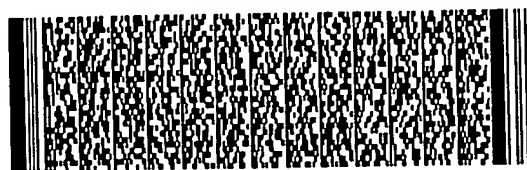
### 實施例

為明顯區別本發明之實施例與傳統技術之差異，茲分別對第1圖中之傳統外接式指紋辨識器與第3圖本發明實施例中之無線指紋辨識裝置進行比較。

請參閱第3圖，第3圖係表示根據本發明實施例中，具有無線指紋辨識裝置之筆記型電腦示意圖。

如第3圖中所示，習知技術中的連接纜線14由無線電波40取代，其所使用的無線傳輸協定可以用一般大家所熟知的藍芽無線傳輸協定，藉此達到標準化、同時降低生產成本的目的。

本發明實施例中無線指紋辨識裝置可透過無線傳輸的方式來進行身份確認，所以當在會議中要使用這筆記型電腦30前進行身份確認時，不用再外接一外接式指紋辨識器13，來進行指紋辨識的工作；由於無線指紋辨識裝置之識



## 五、發明說明 (7)

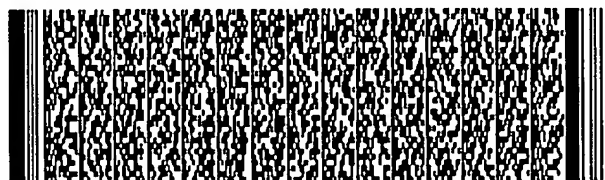
別器20在技術上可做的很小，又具有無線傳輸的功能，使用者只要接近筆記型電腦30，在口袋中將手指按在識別器20的指紋擷取模組21上，即可進行身份確認工作，而且若將識別器20與鑰匙圈等使用者會隨身攜帶的物品相結合，則可避免使用者忘記帶識別器20的狀況發生，也較不易產生遺失的情形。

### 實施例一

請參考第4A圖，第4A圖係表示根據本發明實施例中，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

如第4A圖所示，本發明實施例中之無線指紋辨識裝置，可用在筆記型電腦、桌上型電腦或是其他相關系統上，其具有一識別器20，內含一指紋鑑別模組23，通常是一單晶片微處理器，該指紋鑑別模組23耦接於一指紋擷取模組21、一射頻模組22及一記憶體24，其中指紋擷取模組21可取得使用者的指紋資料，記憶體24可使用電子式可抹除且可程式唯讀記憶體(EEPROM)或是快閃記憶體(Flash memory)，可儲存預設的使用者指紋資料，若上述指紋鑑別模組23比對此指紋資料與預設指紋資料相符時，可透過射頻模組22以藍芽無線傳輸協定或其他無線電方式所傳送一控制訊號。不過為了系統的安全考量，此無線傳輸的有效範圍在10公尺之內。

本發明實施例中之無線指紋辨識裝置具有一接收模組31，可接收藍芽無線傳輸協定或其他無線電方式所傳送之控制訊號，透過此控制訊號來控制筆記型電腦內部晶片組



#### 五、發明說明 (8)

32 啟動筆記型電腦30的電源供應器33或是開放筆記型電腦30之使用權。

請參考第4B圖，第4B圖係表示根據本發明實施例中，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

依據本發明實施例之無線指紋辨識裝置，提供一種無線身份識別方法，包括下列步驟，如第4B圖所示，使用者先在識別器20上建立一預設指紋資料，並將該預設指紋資料儲存於記憶體中(步驟S401)，如電子式可抹除且可程式唯讀記憶體(EEPROM)或是快閃記憶體(Flash memory)。以後，當要使用該筆記型電腦30時(步驟S402)，使用者將手指按在識別器20的指紋擷取模組21上，指紋擷取模組21取得使用者之指紋資料後(步驟S403)，此時指紋鑑別模組23會判斷該指紋資料與預設指紋資料是否相符？(步驟S404)，若該指紋資料與預設指紋資料相符時，透過藍芽無線通訊協定將一控制訊號送出(步驟S405)，無線指紋辨識裝置之接收模組31接到該控制訊號後，透過此控制訊號來控制筆記型電腦內部晶片組32啟動筆記型電腦30的電源供應器33或是開放筆記型電腦30之使用權(步驟S407)。接著便結束指紋辨識流程(步驟S408)，若該指紋資料與預設指紋資料不同時，則清除該指紋資料(步驟S406)，並結束指紋辨識流程(步驟S408)。

#### 實施例二

請參考第5A圖，第5A圖係表示根據本發明第二實施例中，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

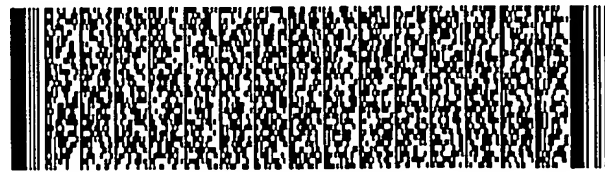


## 五、發明說明 (9)

如第5A圖所示，本發明實施例中之無線指紋辨識裝置，可用在筆記型電腦、桌上型電腦或是其他相關系統上，其具有一識別器20，內含一指紋擷取模組21耦接於一射頻模組22，可取得使用者的指紋資料，並透過射頻模組22以藍芽無線傳輸協定或其他無線電方式傳送該指紋資料，不過為了系統的安全考量，此無線傳輸的有效範圍在10公尺之內。

本發明實施例中之無線指紋辨識裝置是使用在筆記型電腦的身份確認上，在筆記型電腦內部更包括一接收模組31，用以接收藍芽無線傳輸協定或其他無線電方式所傳送之指紋資料。而筆記型電腦內部之指紋鑑別模組34通常是一單晶片微處理器，該指紋鑑別模組34耦接於一接收模組31、一記憶體及筆記型電腦內部之晶片組，其中上述指紋鑑別模組34可單獨形成一模組化設計，或是另設計於筆記型電腦30之主機板上，透過主機板的電路安排連接接收模組31，以降低產品生產成本。上述筆記型電腦內部之記憶體35可使用電子式可抹除且可程式唯讀記憶體(EEPROM)或是快閃記憶體(Flash memory)，可儲存預設的使用者指紋資料，若指紋鑑別模組34比對該指紋資料與該預設指紋資料相符時，則開放筆記型電腦30之使用權；若指紋鑑別模組34比對該指紋資料與該預設指紋資料不符時，則關閉筆記型電腦30。

請參考第5A圖，在本發明實施例中之無線接紋辨識裝置中，指紋鑑別模組34耦接於筆記型電腦內部之晶片組



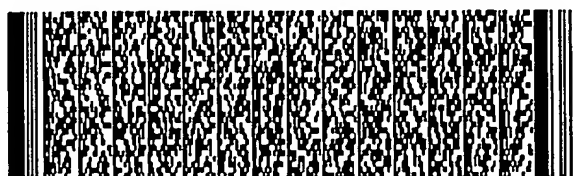
## 五、發明說明 (10)

32，即南橋及北橋晶片組，透過指紋鑑別模組34發出的控制命令給南橋及北橋晶片組，可由筆記型電腦內部之晶片組32控制電源供應器33是否啟動或關閉筆記型電腦30，開放或鎖住筆記型電腦30之使用權或是鎖住筆記型電腦30的鍵盤、滑鼠等輸入裝置。

本發明實施例之另一實施方式，請參考第5B圖，第5B圖係表示根據本發明第二實施例中，具有無線指紋辨識裝置之筆記型電腦，另一實施方式之系統方塊圖。其中筆記型電腦30內部之指紋鑑別模組34可直接耦接於筆記型電腦30內部之電源供應器33，透過指紋鑑別模組34發出的控制命令可直接控制是否啟動或關閉筆記型電腦30。

請參考第5C圖，第5C圖係表示根據本發明第二實施例，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

依據本發明第二實施例之無線指紋辨識裝置，提供一種無線身份識別方法，包括下列步驟，使用者先於識別器20上輸入一預設指紋資料(步驟S501)，經指紋擷取模組21取得後，透過射頻模組22以藍芽無線通訊協定將預設指紋資料傳送給收模組31(步驟S502)，並將該預設指紋資料儲存於筆記型電腦30內部之記憶體35中(步驟S503)，當使用者要使用該筆記型電腦30時(步驟S504)，使用者將手指按在識別器20的指紋擷取模組21上，指紋擷取模組21取得使用者之指紋資料後(步驟S505)，此時，識別器20透過射頻模組22以藍芽無線通訊協定直接將該指紋資料送出(步驟



#### 五、發明說明 (11)

S506)，筆記型電腦30之接收模組31接到該指紋資料後(步驟S507)，指紋鑑別模組34判斷該指紋資料與記憶體35中之預設指紋資料是否相符？(步驟S508) 若該指紋資料與預設指紋資料相符時，則開放筆記型電腦30之使用權(步驟S509)；若該指紋資料與預設指紋資料不相符時，則可關閉筆記型電腦30(步驟S510)，或是直接將鍵盤鎖住，甚至將硬碟資料刪除，以免機密資料洩漏，最後結束指紋辨識流程(步驟S511)。

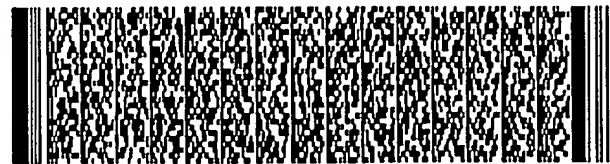
#### 實施例三

請參考第6A圖，第6A圖係表示根據本發明第三實施例，具有無線指紋辨識裝置之筆記型電腦系統方塊圖。

如第6A圖所示，本發明實施例中之無線指紋辨識裝置，可用在筆記型電腦、桌上型電腦或是其他相關系統上，其具有一識別器20，內含一指紋擷取模組21耦接於一射頻模組22，可取得使用者的指紋資料，並透過射頻模組22以藍芽無線傳輸協定或其他無線電方式傳送該指紋資料，不過為了系統的安全考量，此無線傳輸的有效範圍在10公尺之內。

本發明實施例中之無線指紋辨識裝置是使用在筆記型電腦的身份確認上，在筆記型電腦內部更包括一接收模組31，用以接收藍芽無線傳輸協定或其他無線電方式所傳送之指紋資料。

在本發明實施例中，為了節省生產成本，以不在筆記型電腦內部增加一額外單晶片微處理器為原則，而是使用





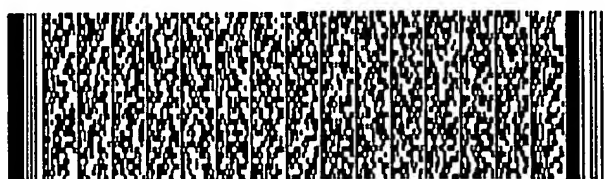
## 五、發明說明 (12)

筆記型電腦的中央處理單元36配合筆記型電腦內部晶片組32，進行指紋鑑別工作。如第6A圖所示，接收模組31與筆記型電腦內部晶片組32耦接，這裡的晶片組32為南橋及北橋晶片組，其另耦接於筆記型電腦之中央處理單元(CPU)36、電源供應器33及一附屬記憶體35，其中此記憶體35可使用主機板上的電子式可抹除且可程式唯讀記憶體(EEPROM)或是額外的附屬記憶體(如快閃記憶體(Flash memory)等)，可儲存預設的使用者的預設指紋資料。

本發明實施例中的筆記型電腦30可在收到識別器20所傳開機指令的一瞬間，若筆記型電腦之中央處理單元36比對指紋資料與預設指紋資料相符時，則透過南橋及北橋晶片組32開放筆記型電腦30之使用權，如：電源供應器33繼續提供電力、開放鍵盤或滑鼠的輸入功能等。若筆記型電腦之中央處理單元36比對指紋資料與預設指紋資料不符時，則立即透過南橋及北橋晶片組32控制電源供應器33關閉筆記型電腦30。

請參考第6B圖，第6B圖係表示根據本發明第三實施例，使用無線指紋辨識裝置之身份識別方法的概略流程圖。

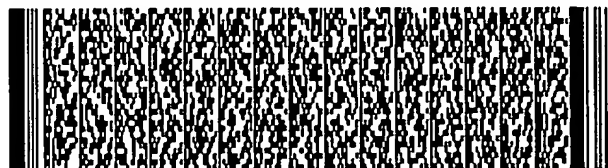
依據本發明第三實施例之無線指紋辨識裝置，提供一種無線身份識別方法，包括下列步驟，如第6B圖所示，使用者先於識別器20上輸入一預設指紋資料(步驟S601)，經指紋擷取模組21取得後，透過射頻模組22以藍芽無線通訊協定將預設指紋資料傳送給收模組31(步驟S602)，並將該



##### 五、發明說明 (13)

預設指紋資料儲存於筆記型電腦30內部之記憶體35中(步驟S603)，當使用者要使用該筆記型電腦30時(步驟S604)，使用者將手指按在識別器20的指紋擷取模組21上，指紋擷取模組21取得使用者之指紋資料後(步驟S605)，此時，識別器20透過射頻模組22以藍芽無線通訊協定直接將該指紋資料送出(步驟S606)，筆記型電腦之接收模組31接到該指紋資料後(步驟S607)，立即啟動筆記型電腦30之電源供應器33，由BIOS先命令南橋及北橋晶片組32將接收模組31所接收之指紋資料傳送至筆記型電腦之中央處理單元36，再與儲存於記憶體35中的預設使用者指紋資料進行比對。此時，筆記型電腦之中央處理單元36會判斷該指紋資料與記憶體35中的預設指紋資料是否相符(步驟S608)？若該指紋資料與預設指紋資料相符時，則透過南橋及北橋晶片組32開放筆記型電腦30之使用權(步驟S609)；若該指紋資料與預設指紋資料不相符時，則可透過南橋及北橋晶片組32依正常程序關閉筆記型電腦30(步驟S610)，或是直接將鍵盤鎖住，甚至將硬碟資料刪除，以免機密資料洩漏，最後結束指紋辨別流程(步驟S611)。

雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。



## 六、申請專利範圍

1. 一種電子系統之指紋辨識裝置，包括：

一識別器，具有一指紋鑑別模組耦接於一指紋擷取模組、一射頻模組及一記憶體，其中該指紋擷取模組可取得一指紋資料，該記憶體用以儲存一預設指紋資料，若該指紋鑑別模組比對該指紋資料與該預設指紋資料相符時，可透過該射頻模組以一無線傳輸協定傳送一控制訊號；以及

一接收模組，用以接收該無線傳輸協定所傳送之該控制訊號，並對該電子系統作一對應控制。

2. 如申請專利範圍第1項所述之指紋辨識裝置，其中該無線傳輸協定為藍芽無線傳輸協定。

3. 如申請專利範圍第1項所述之指紋辨識裝置，其中該指紋鑑別模組為一單晶片微處理器。

4. 如申請專利範圍第1項所述之指紋辨識裝置，其中該記憶體為一快閃記憶體(Flash memory)。

5. 如申請專利範圍第1項所述之指紋辨識裝置，其中該記憶體為一電子式可抹除且可程式唯讀記憶體(EEPROM)。

6. 如申請專利範圍第1項所述之指紋辨識裝置，其中該對應控制為啟動該電子系統。

7. 如申請專利範圍第1項所述之指紋辨識裝置，其中該對應動作為開放該電子系統之使用權。

8. 一種電子系統之指紋辨識裝置，包括：

一識別器，具有一指紋擷取模組，耦接於一射頻模組，該指紋擷取模組可取得一指紋資料，並透過該射頻模



## 六、申請專利範圍

組以一無線傳輸協定傳送該指紋資料；以及

一接收模組，用以接收該無線傳輸協定所傳送之該指紋資料；

一指紋鑑別模組，耦接於該接收模組及一記憶體，其中該記憶體用以儲存一預設指紋資料，該指紋鑑別模組可對該指紋資料與該預設指紋資料進行比對，並對該電子系統作一對應控制。

9. 如申請專利範圍第8項所述之指紋辨識裝置，其中該無線傳輸協定為藍芽無線傳輸協定。

10. 如申請專利範圍第8項所述之指紋辨識裝置，其中該指紋鑑別模組為一單晶片微處理器。

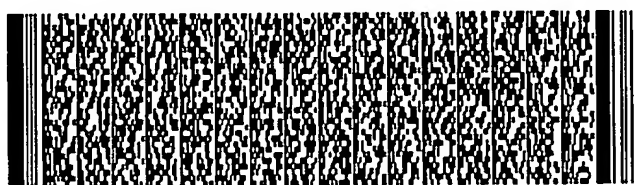
11. 如申請專利範圍第8項所述之指紋辨識裝置，其中該記憶體為一快閃記憶體(Flash memory)。

12. 如申請專利範圍第8項所述之指紋辨識裝置，其中該記憶體為一電子式可抹除且可程式唯讀記憶體(EEPROM)。

13. 如申請專利範圍第8項所述之指紋辨識裝置，其中若該指紋資料與該預設指紋資料相符時，該對應動作為開放該電子系統之使用權。

14. 如申請專利範圍第8項所述之指紋辨識裝置，其中若該指紋資料與該預設指紋資料不相符時，該對應動作為鎖住該電子系統之使用權。

15. 如申請專利範圍第8項所述之指紋辨識裝置，其中若該指紋資料與該預設指紋資料不相符時，該對應動作為



## 六、申請專利範圍

關閉該電子系統。

16. 如申請專利範圍第8項所述之指紋辨識裝置，其中該電子系統為筆記型電腦。

17. 如申請專利範圍第16項所述之指紋辨識裝置其中該指紋鑑別模組包括該筆記型電腦之一中央處理單元及該筆記型電腦之一晶片組。

18. 一種無線身份識別方法，適用於一電子系統，包括下列步驟：

A. 設定一預設指紋資料；

B. 取得一指紋資料；

C. 比對該預設指紋資料與該指紋資料；以及

D. 若該指紋資料與預設指紋資料相符時，則透過一無線通訊協定傳送一第一控制訊號。

19. 如申請專利範圍第18項所述之無線身份識別方法，其中該無線傳輸協定為藍芽無線傳輸協定。

20. 如申請專利範圍第18項所述之無線身份識別方法，其中該控制訊號用以啟動該電子系統。

21. 如申請專利範圍第18項所述之無線身份識別方法，其中該控制訊號用以開放該電子系統之使用權。

22. 如申請專利範圍第18項所述之無線身份識別方法，更包括下列步驟：

E. 若該指紋資料與該預設指紋資料不相符時，則送出一第二控制訊號。

23. 如申請專利範圍第22項所述之無線身份識別方



#### 六、申請專利範圍

法，其中該第二控制訊號用以關閉該電子系統。

24. 如申請專利範圍第22項所述之無線身份識別方法，其中該第二控制訊號用以鎖住該電子系統之使用權。

25. 一種無線身份識別方法，適用於一電子系統，包括下列步驟：

- A. 設定一預設指紋資料；
- B. 取得一指紋資料；
- C. 透過一無線通訊協定傳送該指紋資料；以及
- D. 比對該預設指紋資料與該指紋資料。

26. 如申請專利範圍第25項所述之無線身份識別方法，其中該無線傳輸協定為藍芽無線傳輸協定。

27 如申請專利範圍第25項所述之無線身份識別方法，更包括下列步驟：

E. 若該指紋資料與該預設指紋資料相符時，則送出一第一控制訊號。

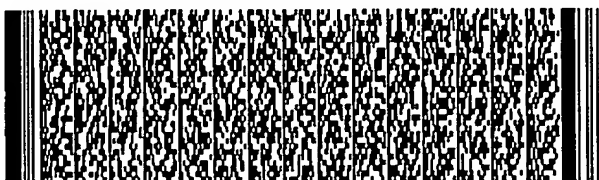
28. 如申請專利範圍第27項所述之無線身份識別方法，其中該第一控制訊號用以啟動該電子系統。

29. 如申請專利範圍第27項所述之無線身份識別方法，其中該第一控制訊號用以開放該電子系統之使用權。

30. 如申請專利範圍第25項所述之無線身份識別方法，更包括下列步驟：

F. 若該指紋資料與該預設指紋資料不相符時，則送出一第二控制訊號。

31. 如申請專利範圍第30項所述之無線身份識別方

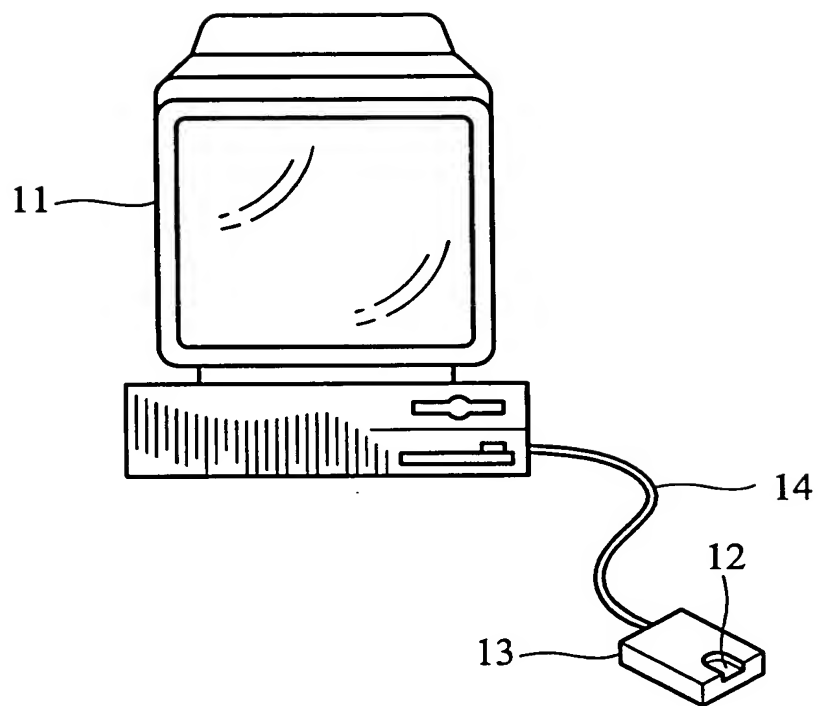


六、申請專利範圍

法，其中該第二控制訊號用以關閉該電子系統。

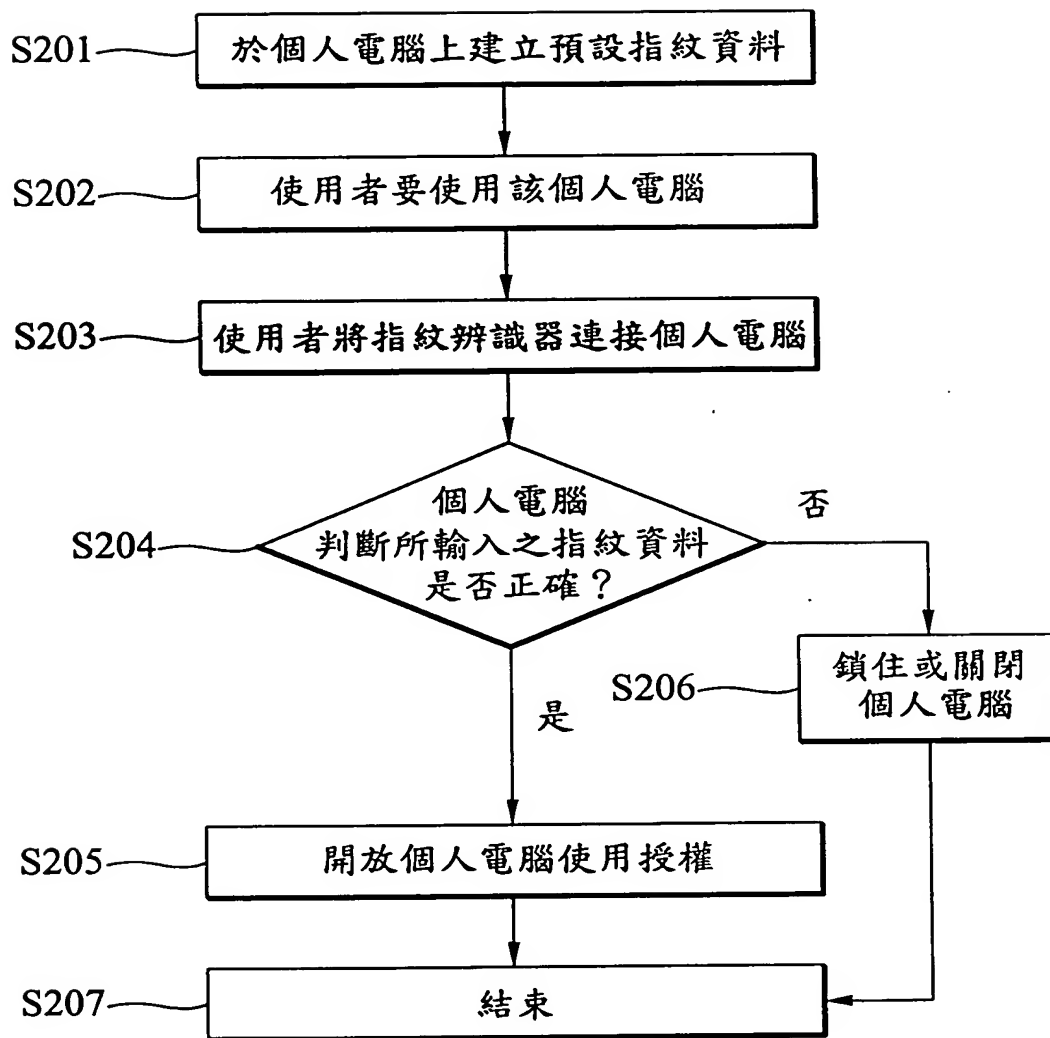
32. 如申請專利範圍第30項所述之無線身份識別方法，其中該第二控制訊號用以鎖住該電子系統之使用權。



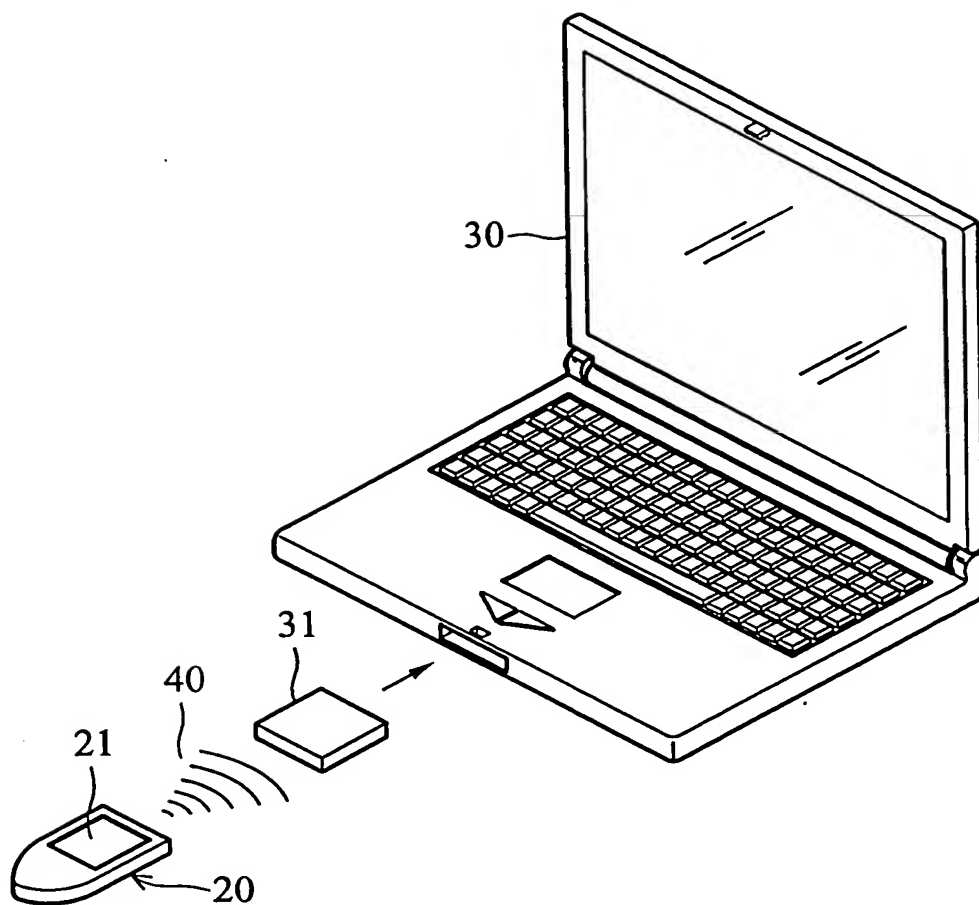


第 1 圖

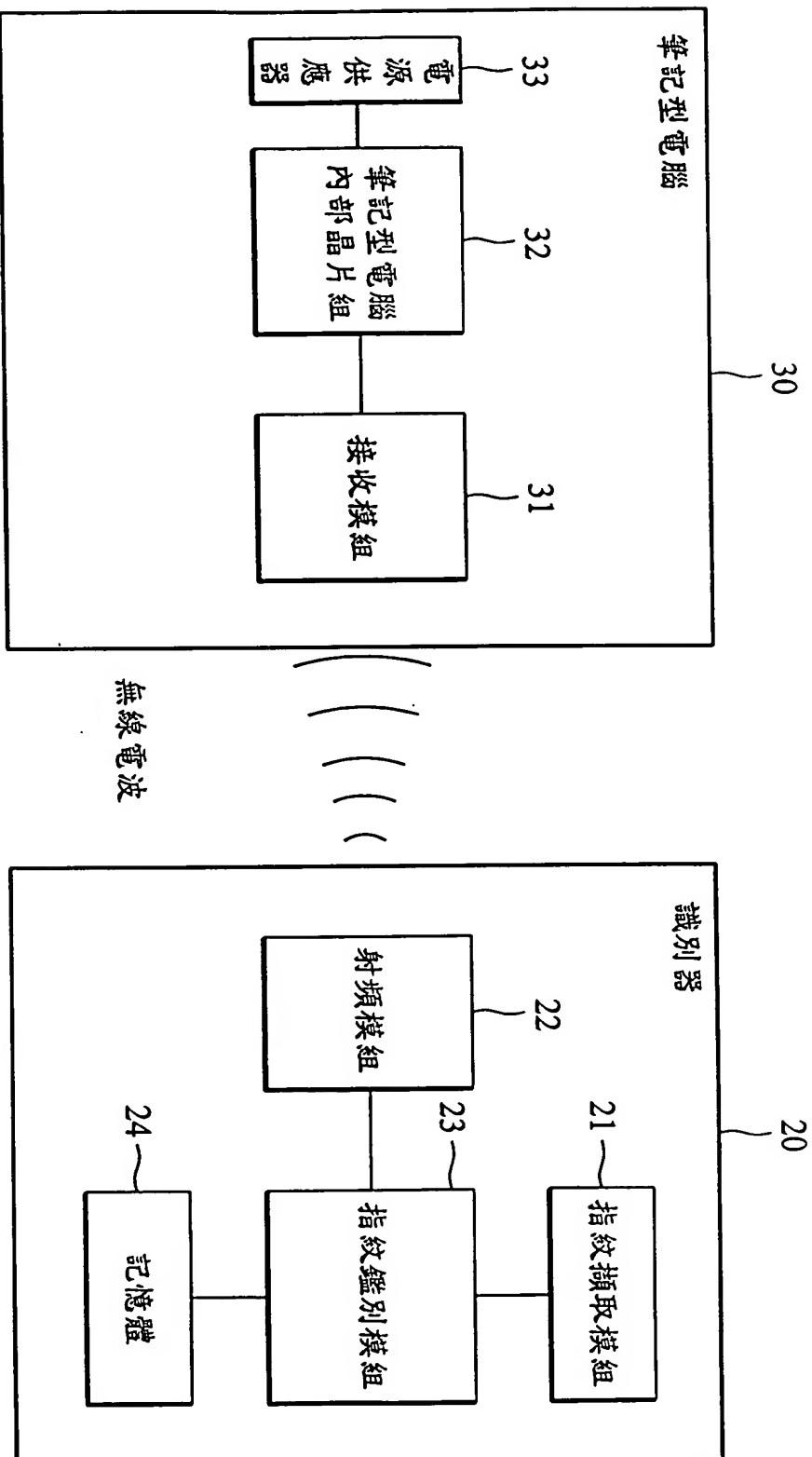




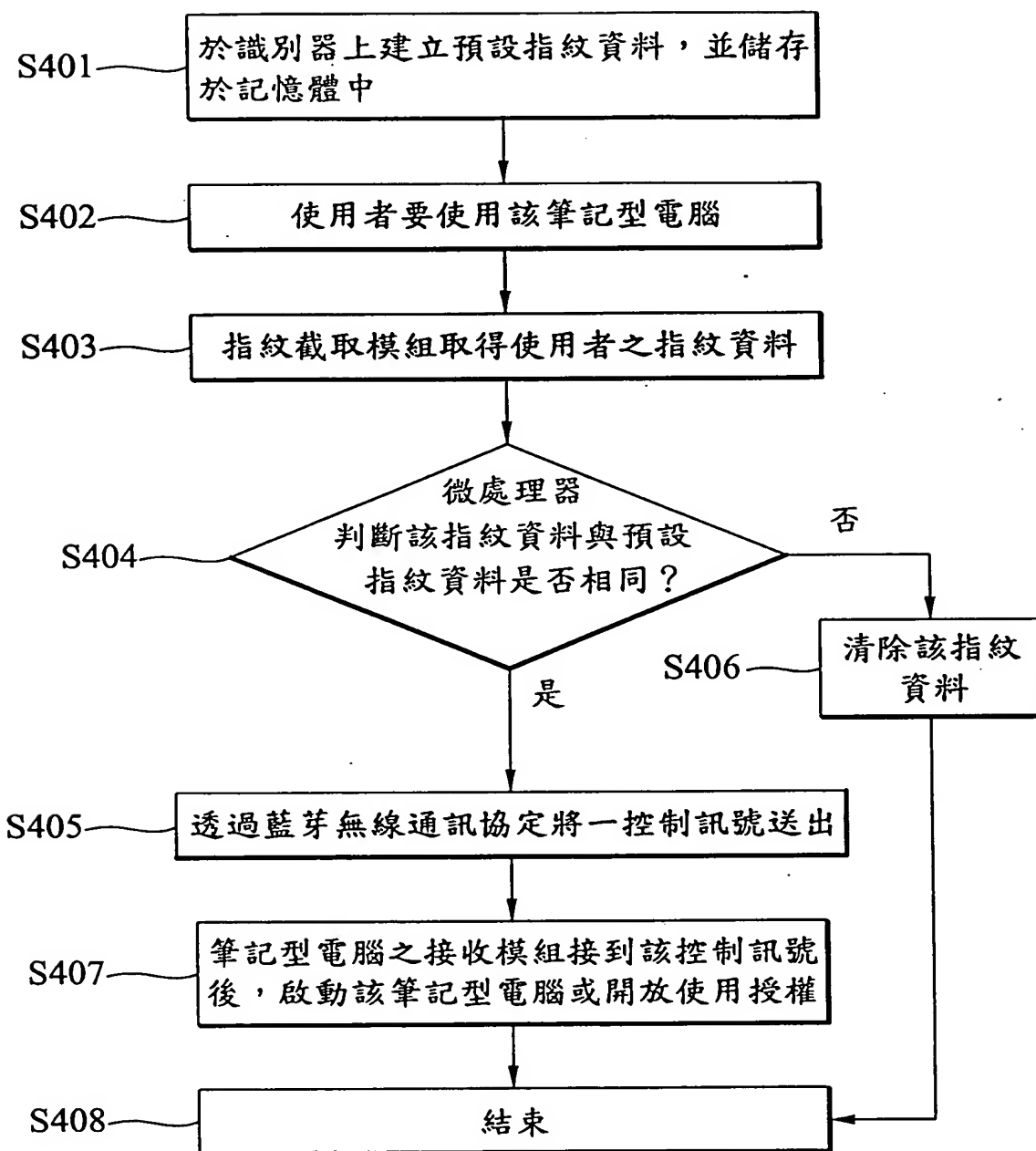
第 2 圖



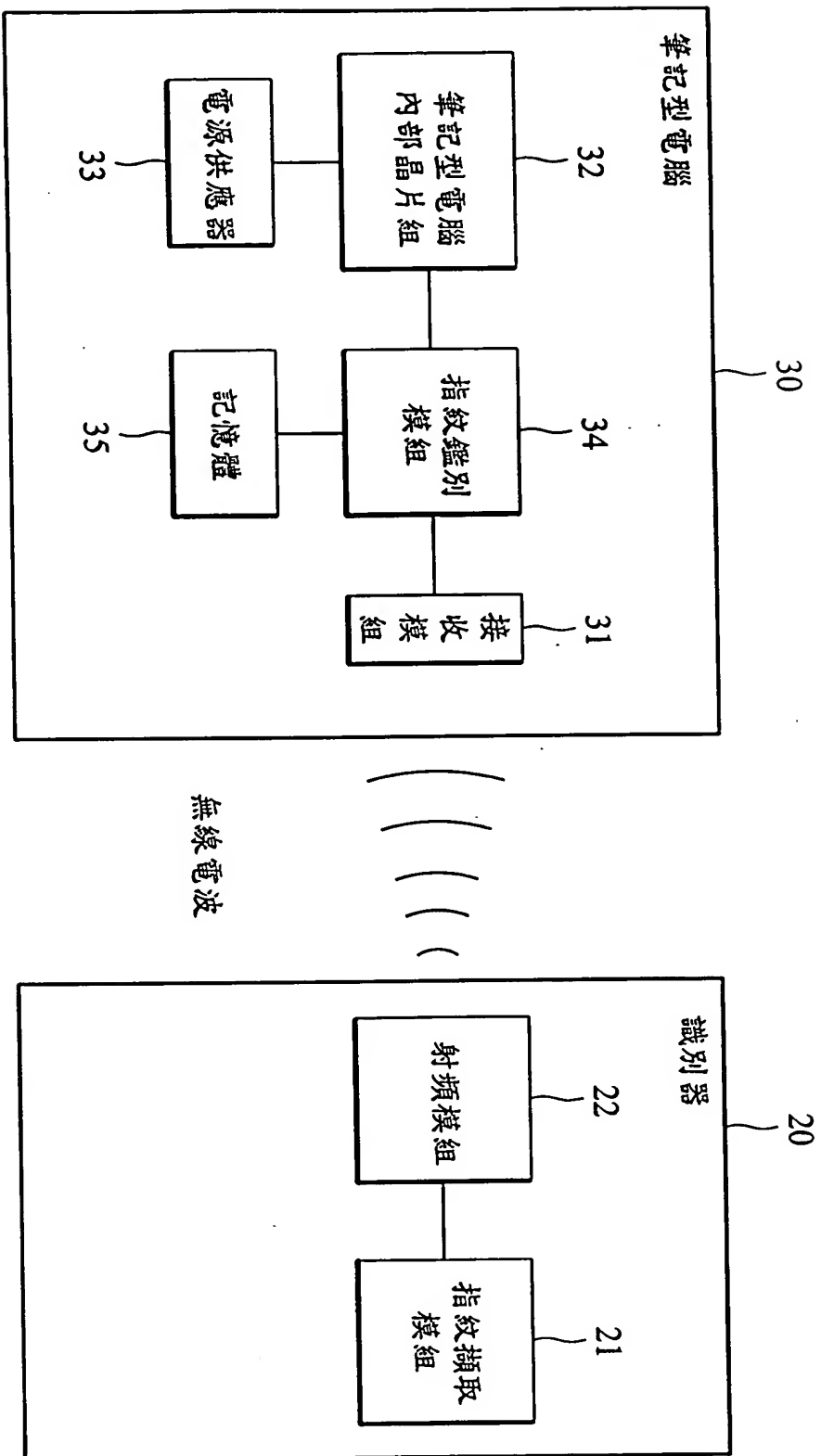
第 3 圖



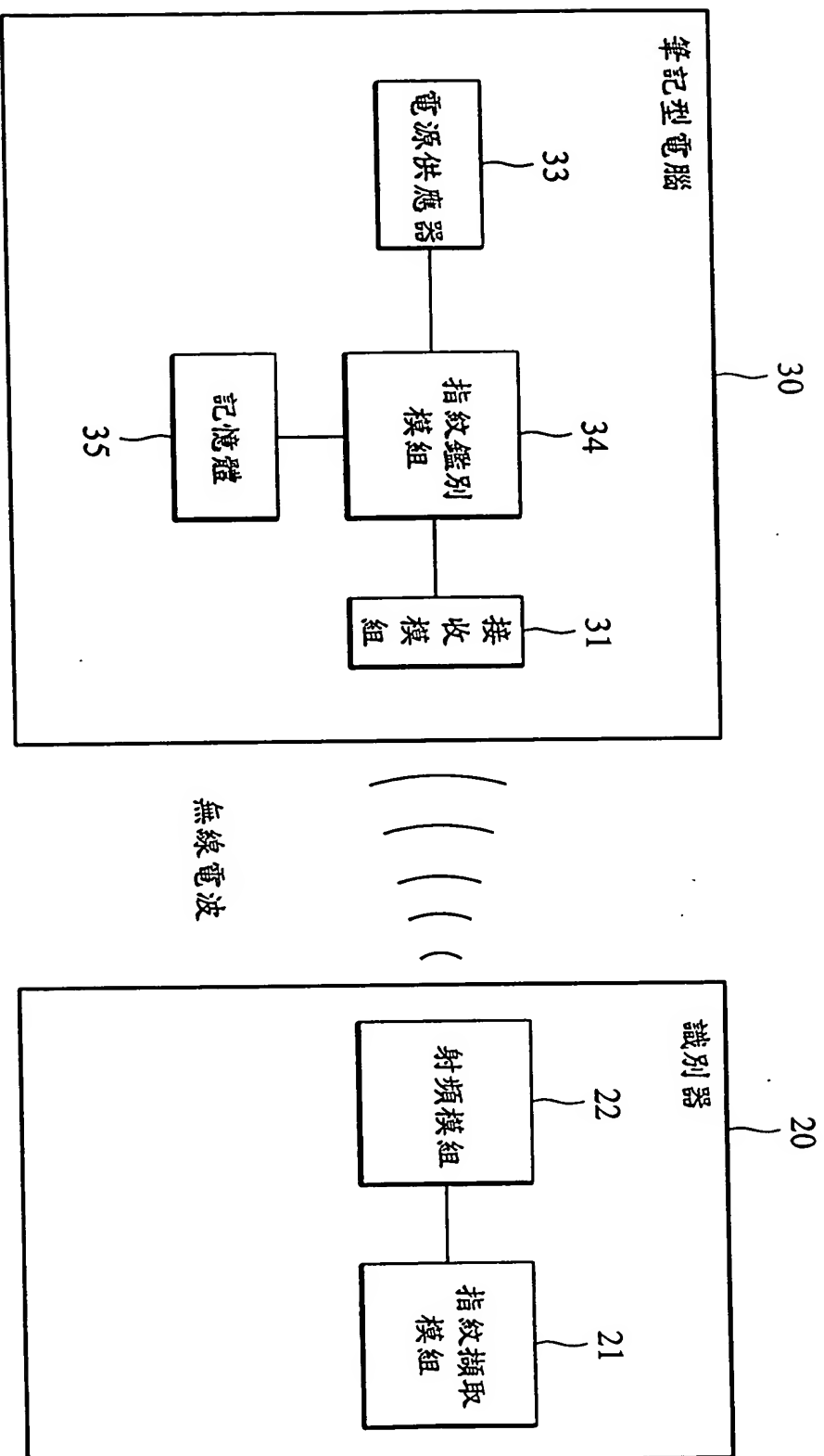
第4A圖



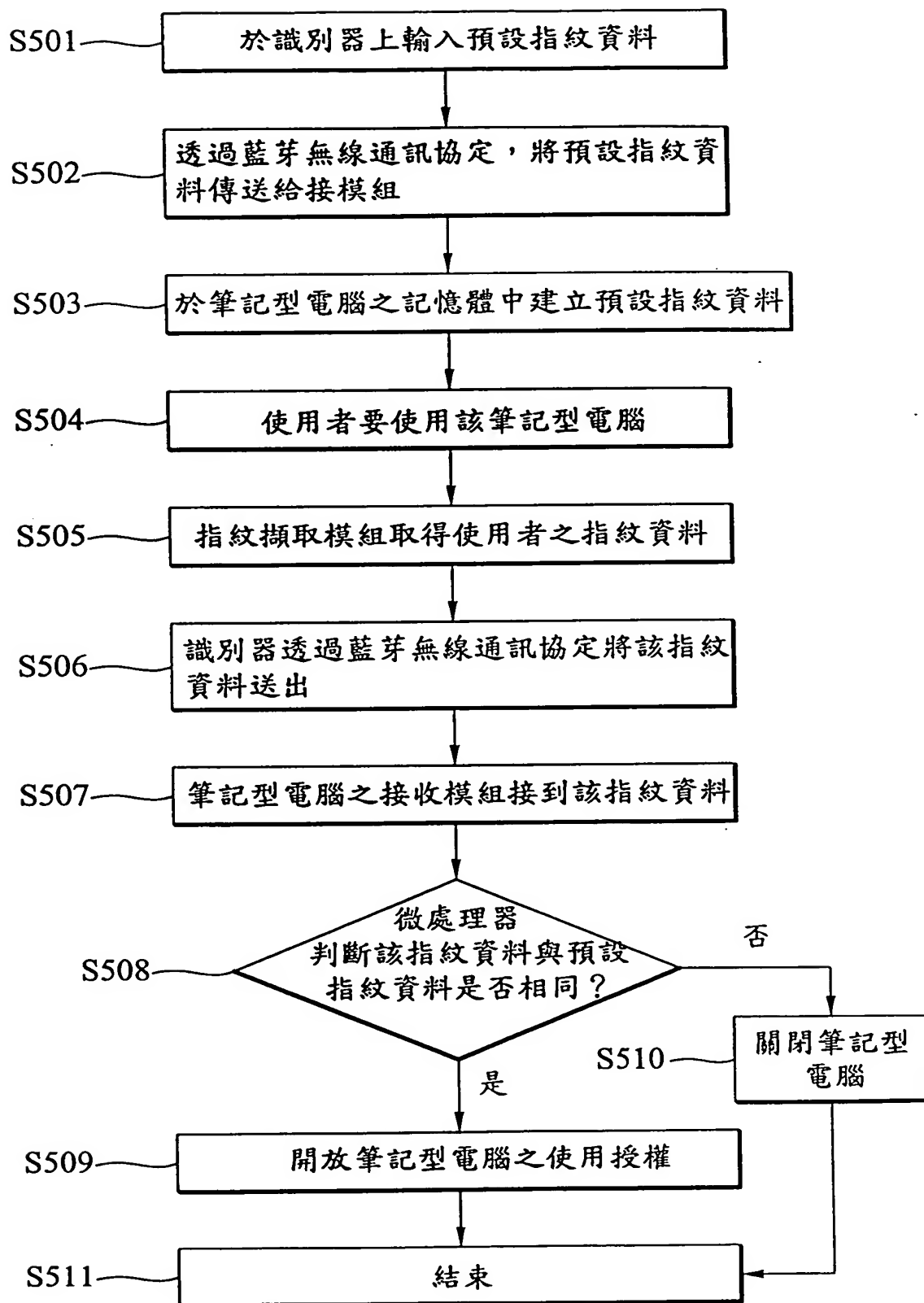
第4B圖



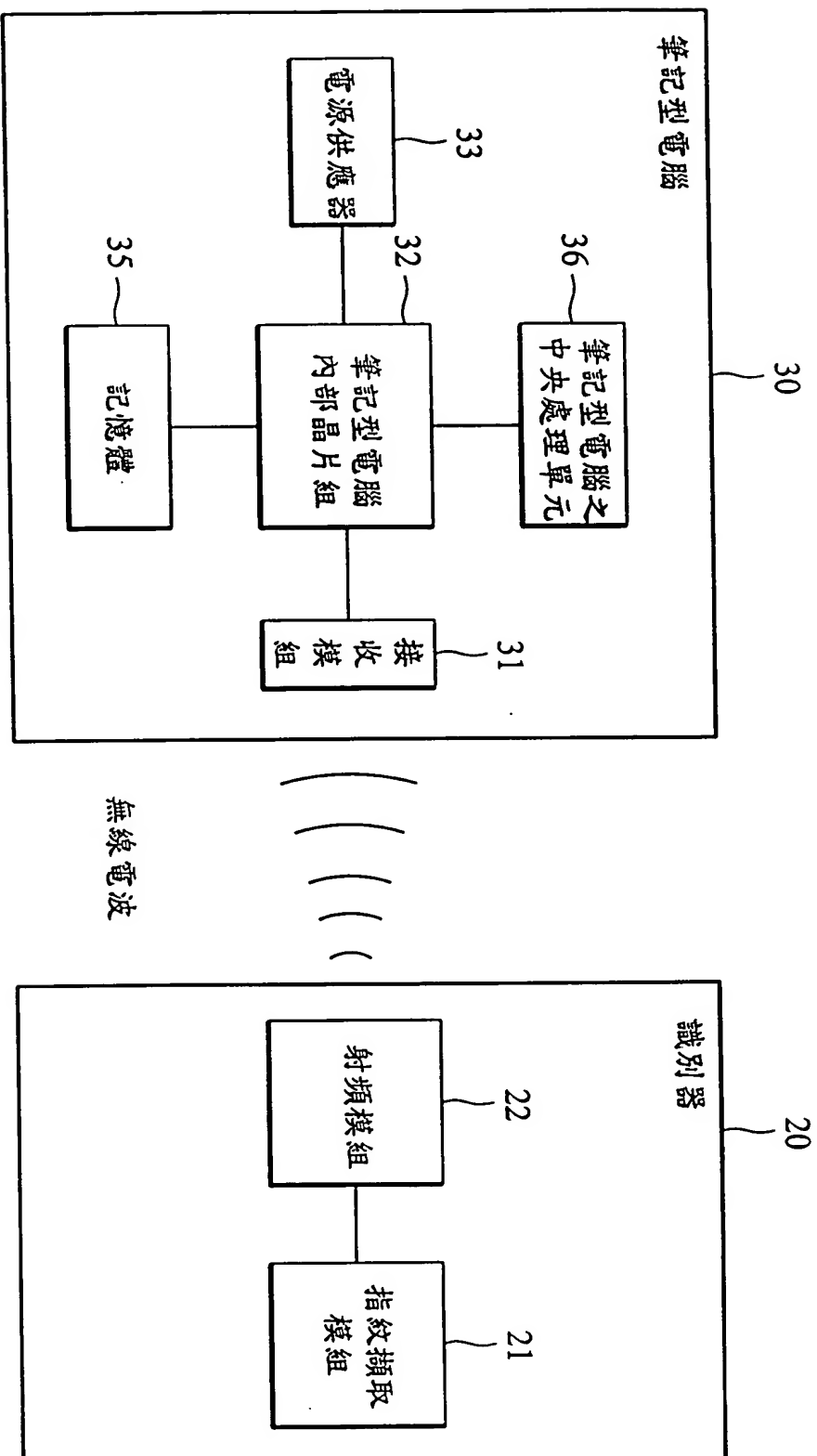
第5A圖



第5B圖

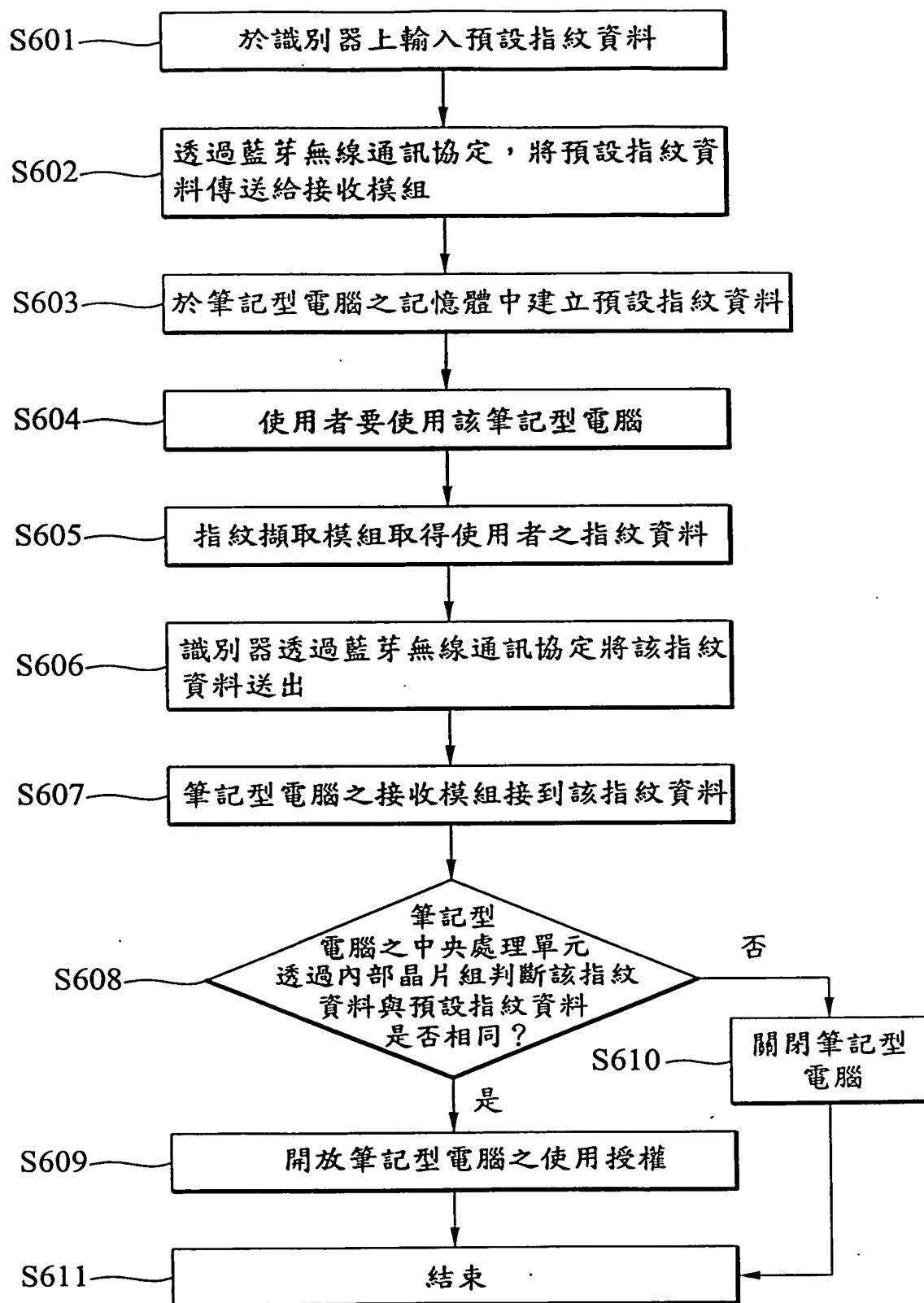


第5C圖



第6A圖





第6B圖

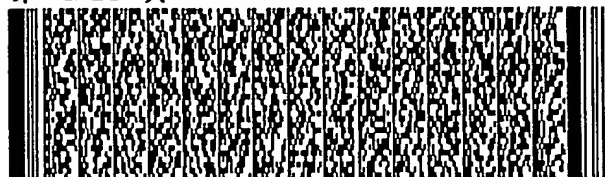
第 1/21 頁



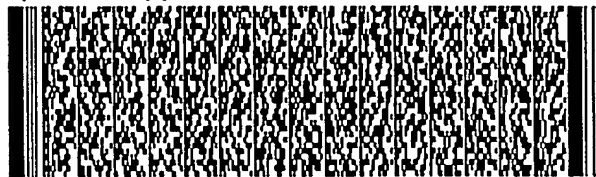
第 2/21 頁



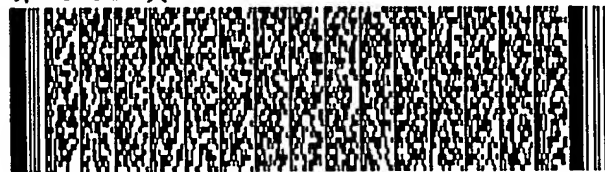
第 4/21 頁



第 4/21 頁



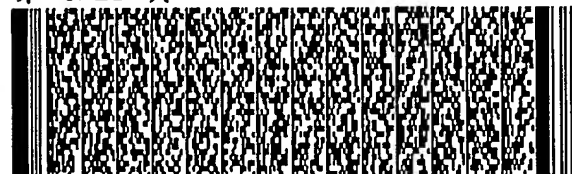
第 5/21 頁



第 5/21 頁



第 6/21 頁



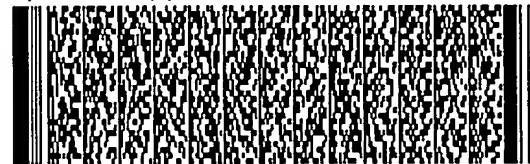
第 6/21 頁



第 7/21 頁



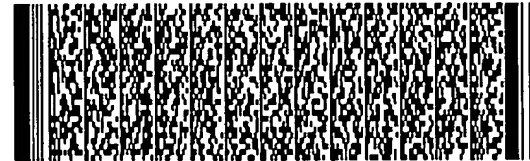
第 7/21 頁



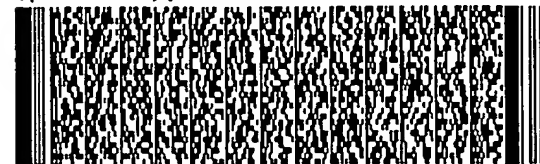
第 8/21 頁



第 9/21 頁



第 9/21 頁



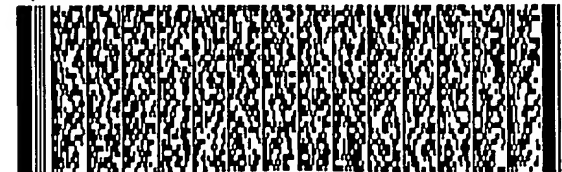
第 10/21 頁



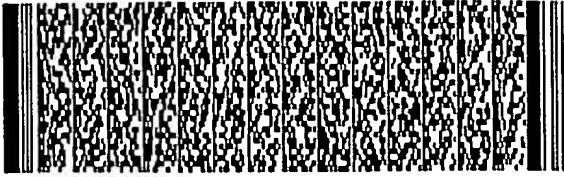
第 10/21 頁



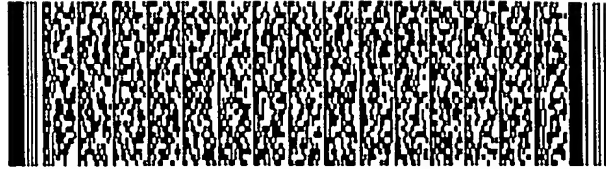
第 11/21 頁



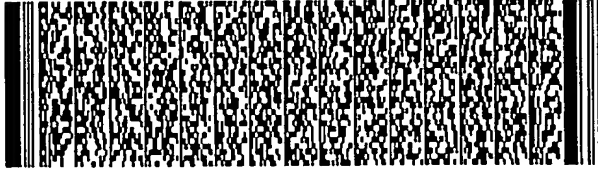
第 11/21 頁



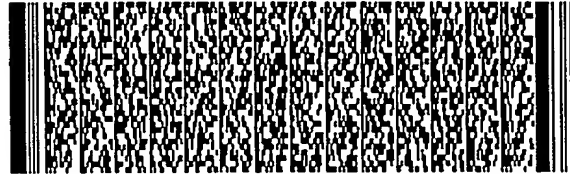
第 12/21 頁



第 12/21 頁



第 13/21 頁



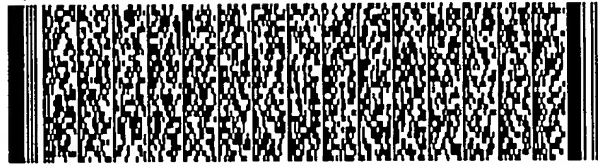
第 13/21 頁



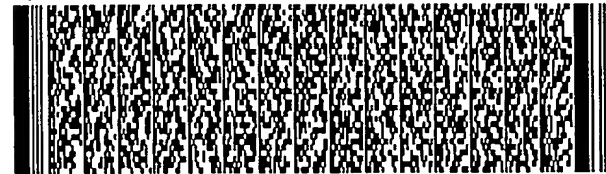
第 14/21 頁



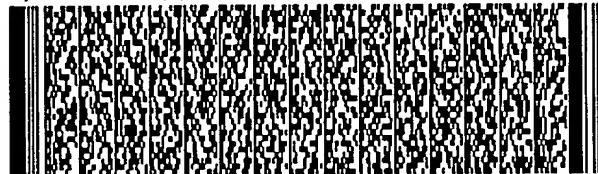
第 14/21 頁



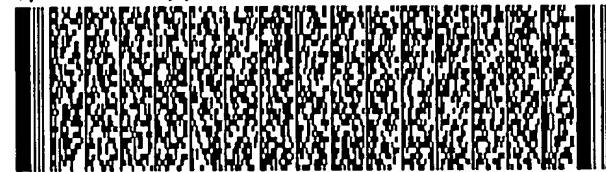
第 15/21 頁



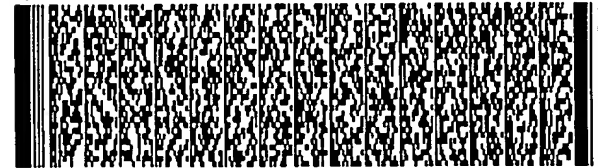
第 15/21 頁



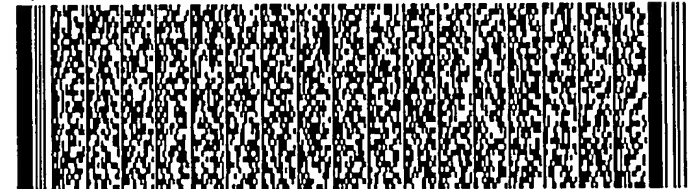
第 16/21 頁



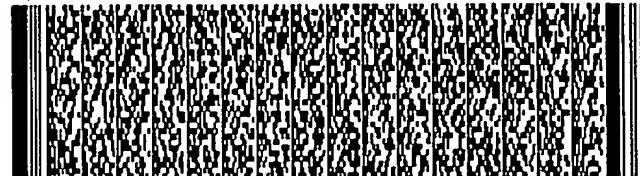
第 16/21 頁



第 17/21 頁



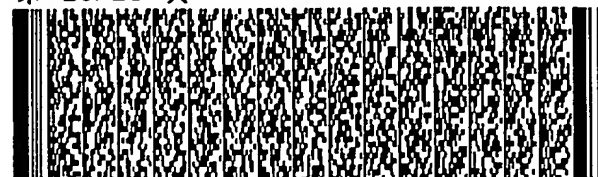
第 18/21 頁



第 19/21 頁



第 20/21 頁



第 21/21 頁



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**